Joint Enterprise Defense Infrastructure (JEDI) Cloud
DRAFT Statement of Objectives (SOO)

Updated 5 March 2018

0 Introduction

The Department of Defense (Department)'s lack of a coordinated enterprise-level approach to cloud infrastructure makes it virtually impossible for our warfighters and leaders to make critical data-driven decisions at "mission-speed", negatively affecting outcomes. In the absence of modern services, warfighters and leaders are forced to choose between foregoing capabilities or slogging through a lengthy acquisition, rollout, and provisioning process. A fragmented and largely on-premise computing and storage solution forces the warfighter into tedious data and application management processes, compromising their ability to rapidly access, manipulate, and analyze data at the home front and tactical edge. Most importantly, current environments are not optimized to support large, cross domain analysis using advanced capabilities such as machine learning and artificial intelligence to meet current and future warfighting needs and requirements.

Increasingly sophisticated cyber attacks from multiple adversaries, known and unknown, demand that the Department develop an updated security framework. There is a clear and immediate need for repeatable, verifiable, and measurable security from the physical level, through the logical layer, and down to the datasets.

This Statement of Objectives (SOO) describes the Department's intentions for the Joint Enterprise Defense Infrastructure (JEDI) Cloud program and for the supporting contract to acquire commercial infrastructure as a service (IaaS) and platform as a service (PaaS) offerings. It is issued with the intent of maximizing offeror flexibility in developing solutions to meet DoD's objectives.

1 Purpose

The purpose of this SOO is to enable the acquisition of modern, enterprise-level cloud services in support of Department related missions and projects from a Cloud Service Provider (CSP) with an existing, large, globally available public offering.

2 Scope

The JEDI Cloud program will provide enterprise-level, commercial cloud services as Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) to the U.S. Department of Defense and related mission partners. Meaning the JEDI Cloud users (referred to as DoD below)

could include: all of U.S. Department of Defense, including all branches of the military -- Army, Navy, Marine Corps, Air Force; the Defense Intelligence community; and the Fourth Estate; as well as the U.S. Coast Guard.

JEDI Cloud service will be offered at all classification levels, across the home front to the tactical edge, including disconnected and austere environments, and closed loop networks. Further, JEDI Cloud service must be able to produce industry standard metrics demanded by present-day battles.

There are eight primary objectives that the acquired cloud solution must achieve:

2.1 Globally Available Services

A worldwide, highly available, resilient infrastructure supporting geographically dispersed users across the homefront to the tactical edge, including austere and connectivity deprived environments, at all classification levels. Additionally, standalone computing and storage resources that can be used in closed-loop networks to support warfighter operations and then seamlessly re-integrate with the global infrastructure.

2.2 Accessible

A secure and reliable cloud services solution accessible to users across the homefront to the tactical edge, including austere and connectivity deprived environments, at all classification levels, that provides automated failover and enables interoperability between applications and access to data.

2.3 Centralized Management and Distributed Control

A solution that enables a central Cloud Computing Program Office (CCPO) to exert appropriate oversight and management of cloud services for the DoD, including applying security policies; monitoring security compliance and service usage across the network; and accrediting standardized service configurations. To automate, to the extent possible, and distribute the account provisioning process, including the management of budgets and expenditures, from the CCPO to users.

2.4 Ease of Use

A solution that decreases the technical expertise required to effectively store data and access, deploy, and manage applications using cloud services. Efficient self-service and initiation of computing and storage services enabling rapid development and deployment of new

applications and advanced capabilities. Enables a method for migrating both modern and re-engineered legacy systems and applications.

2.5 Commercial Parity

Parity with commercially available cloud service offerings where the services available to DoD keep pace with advancements in industry and new features are rapidly made available to DoD as they become commercially available.

2.6 Modern and Elastic Computing, Storage and Network Infrastructure

Provisions modern computing, storage and network infrastructure that is updated and maintained regularly -- including processing architectures, servers, storage options, and platform software -- and with scale to meet consumption to enable rapid development and deployment in support of mission needs.

2.7 Fortified Security

Security that enables enhanced cyber defenses from the root level of systems through the application layer and down to the data layer with improved capabilities including continuous monitoring and auditing, automated threat identification, resiliency against persistent adversary threat, and an operating environment that meets or exceeds DoD information security requirements.

2.8 Advanced Data Analytics

An environment that securely enables data-driven and timely decision making at the tactical level (within a single data domain) and strategic level (across data domains) and supports advanced data analytics capabilities such as machine learning and artificial intelligence.

3 Performance Objectives

The objectives in this section are a desired capability, condition, or attribute of JEDI Cloud. Unless otherwise annotated the stated objectives apply across all domains of classification. The Government understands that various Cloud Service Providers (CSP) may propose additional functionality as part of their Cloud Service Offering (CSO) and does not want to limit potential functionality within the proposed solution. The objectives outlined below must be available and meet accreditation and authorization requirements within 30 days of contract award for unclassified services; within 6 months of contract award for classified services at the Secret level; and within 9 months of contract award for classified services at the Top

Secret/Sensitive Compartmented Information (TS/SCI) and Special Access Program (SAP) levels.

3.0 Provide a “tactical edge” computing and storage capability which is durable, ruggedized, and portable.

3.1 Provide the ability for JEDI Cloud to scale, in the continental United States (CONUS) and outside the continental United States (OCONUS). Scalability should improve computing and storage capacity, efficiently and rapidly, to meet mission requirements.

3.2 Provide robust network capacity, suitable for handling a high volume of traffic globally, in and out of the provider’s cloud boundary. This capacity should be commensurate with the provider’s public offering.

3.3 Computing and storage capability at the “tactical edge” should be able to automatically synchronize with connected JEDI Cloud regions, integrating new data and analysis generated while “disconnected”, once network connectivity is re-established.

3.4 Provides dynamic scalability and resiliency through industry standard mechanisms.

3.5 Service providers should provide the ability to monitor and audit service health and security, including all data pipelines, with an easy to use, intuitive application.

3.6 Individual cloud service offerings from the catalog of available services should be able to be authorized and deauthorized for use by the entire Department or individual organizations within it by the CCPO.

3.7 Provide a mechanism for role-based access control (RBAC) within an account to include account administration, provisioning of new cloud services, and management of existing services.

3.8 Provide a mechanism to deploy cloud-based computing and storage services based on standardized configurations and security policies where appropriate, and a simple mechanism to deprovision any service.

3.9 Provide a mechanism to securely verify user identity using modern authentication protocols including multi-factor authentication (MFA) and public key infrastructure (PKI) that works in all supported environments.

3.10 Provide a mechanism to federate identity including time-limited, role-based authentication tokens which works in all supported environments.

3.11 Provide cloud-service usage reports per entire contract, per account, and specific DoD organizations.

3.12 Provide the ability to rapidly deploy IaaS and PaaS offerings from an online marketplace with baseline template configurations where appropriate.

3.13 Standard and easy to interpret logs, for both humans and machines for tracking of provisioning of services, configuration changes, service access and errors, and any relevant audit trail events.

3.14 Provide a pricing calculator with realistic, accurate, and easy to perform cost modeling and projection.

3.15 Should provide easy to understand training materials and documentation that facilitates making use of services.

3.16 Allow users to rapidly deploy third party platform and software services with integrated billing in a self-service manner.

3.17 Provide processing unit architectures, system memory, storage capabilities, and networking options that are optimized for specific compute-based IaaS activities required by the DoD.

3.18 Provide online, nearline, and offline storage options at the scale and speed to meet mission requirements.

3.19 Provide modern, advanced data analytics tools including machine learning and artificial intelligence capabilities.

3.20 Provide reports, as needed, on infrastructure hosting DoD systems, including specific server hardware, network systems, power infrastructure, cooling systems, etc and software running on those systems below the virtualization layer across the enterprise.

3.21 Provide a range of service pricing structures that incorporate both usage-based pricing to incentivize efficient utilization of cloud computing resources and subscription models for reserved resources.

3.22 Provide specific standards required to utilize commercial cloud services.

4 Performance Requirements

The requirements in this section are a minimum capability, condition, or attribute of JEDI Cloud. Unless otherwise stated, all requirements apply across all domains of classification. The Government understands that various CSPs may propose additional functionality as part of their CSO and does not want to limit potential functionality within the proposed solution. All time-based requirements identified below exist for CONUS, OCONUS, and disconnected (tactical edge) instances where appropriate. The requirements outlined below must be available and meet accreditation and authorization requirements within 30 days of contract award for unclassified services; within 6 months of contract award for classified services at the Secret level; and within 9 months of contract award for classified services at the Top Secret/Sensitive Compartmented Information (TS/SCI) and Special Access Program (SAP) levels.

4.0 For all networks operating above the unclassified level the network must be a closed-loop system.

4.1 Meet all security related objectives outlined in the JEDI Cloud Cyber Security Plan.

4.2 Provide a user interface to track budgets, including spend reports, cost planning and projections, and setting limits based on cloud service usage both for individual accounts and at the DoD level, including notifications and alerts where appropriate.

4.3 Provide an application program interface (API) with access to service usage, actual costs, and the ability to set budget limits with notifications for individual accounts and across the enterprise.

4.4 All billing reports and invoices must identify most significant cost drivers.

4.5 Provisioning a new account, user, service offering or deploying said offerings within the DoD cloud must not take any longer than what is offered through commercial access.

4.6 Provide an API that supports the creation, listing, reading, updating, or deletion of accounts, users, roles, and services, including any available CSP-native computing or storage offerings and network configuration.

4.7 Provider must continue to have a commercial public offering. The Department's usage should not exceed 50% of the total capacity of the provider's infrastructure, including network traffic, online/nearline/offline storage, and compute. The Provider shall provide this information as part of the Monthly Report.

4.8 Generational replacement and upgrading of all hardware (compute, memory, storage, and networking) must be on par with the commercial (non-government) offering of the provider. When upgrading hardware, the new generation must be on par with commercially available offerings in all cases.

4.9 The response time for confirmation of job submission on any IaaS offering deployment should be on the order of seconds and the initiation of that request must be on the order of seconds to a few minutes.

4.10 The time required to go from power off to receiving user instructions for an individual IaaS compute instance must be on the order of seconds.

4.11 The provider must have more than one online database storage offering that can support data on the order of hundreds of Terabytes and can be queried in under one second.

4.12 The provider must have at least one online object storage offering that can support data on the order of Petabytes.

4.13 The provider must offer data storage solutions that include both traditional relational databases and recent alternatives (so-called “noSQL” databases). Versions of such database management systems (DBMS) must stay current with all major releases of those DBMSs.

4.14 There must be options for “nearline” (versus online/offline) storage solutions. Such options must provide read and write access on the order of minutes.

4.15 There must be options for “offline” storage solutions. Such options must provide read and write access on the order of many minutes up to a few hours.

4.16 New cloud service offerings that the provider makes commercially available must be available to the Department immediately upon internal DoD approval at each classification level.

4.17 The Department must have a mechanism for activating and deactivating any cloud service offering for the entire enterprise, an individual account, or any number of accounts.

4.18 The provider’s networking hardware, including links, endpoints, and pass-throughs, must keep pace with commercially available networking hardware. Network capacity, as measured by throughput and latency, must keep pace with commercial norms and expectations.

4.19 Upon notification of the Contracting Officer, the vendor must provide a portability plan. (CLIN x004). The portability plan must specifically identify, in the form of user instructions, the complete set of processes and procedures that are necessary to extract all online, nearline, and offline data, including, but not limited to, databases, object and file storage, system configurations, and network configurations such that any DoD customer can use these instructions to migrate from JEDI Cloud to another environment. The portability plan must also include an explanation evidencing the ability to demonstrate successful cleansing or destruction of all system components and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once removed from JEDI Cloud. Furthermore, the vendor must demonstrate migration of an application and data (provided by the Government for this purpose) from JEDI Cloud to a different hosting environment. The demonstration shall validate the user instructions and evidence a reasonable ability to successfully migration off of JEDI Cloud.

4.20 Provide usage reports that contain service usage for all billable aspects offered by the Provider. This information should be produced at the account level, available on all classification levels, and easily aggregated to a Departmental (enterprise) level.

4.21 Provides dynamic scalability and resiliency through industry standard mechanisms, including the ability for users to create system configurations that are tolerant against catastrophic data center loss by failing over to another availability zone.

4.22 Provide advanced data analytics service offerings, to include machine learning and artificial intelligence, available in all environments, including classified regions and disconnected environments. Such offerings must be able to operate across multiple datasets in disparate accounts under the Departmental enterprise organization.

4.23 All actions in the system must be loggable, whether by a human or a machine, to an external, non-overwritable destination also within the cloud provider. Such logs must be sufficient to provide an audit trail of activities and actions as required in accordance with the November 17, 2017 memo, Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings.

4.24 The provider must have an online marketplace within the cloud environment that supports end users deploying service offerings both native to the CSP and from third party vendors. Deploying an offering from this marketplace must be achievable within 5 minutes of authentication into the cloud environment user interface.

4.25 The provider must be able to support the deployment of platforms and software where the Department already possesses a license using a "Bring your own license" approach. This must be integrated with the online marketplace.

4.26 The provider must provide the Department with access to the latest advances in processing architectures, or similar emerging compute capability as is commercially available via service offerings within the cloud environment.

4.27 The Provider shall provide a program management capability to effectively oversee all contract activities. The provider shall appoint a Program Manager (PM) with sufficient expertise and authority to execute the following responsibilities: serve as the official interface between the provider and the Sponsor to be available as needed for sponsor interaction, and monitor and report on contract status and Service Level Agreements (SLA).

4.28 Upon notification of the Contracting Officer, the vendor must provide a transition plan. (CLIN x005). The transition plan must specifically identify, in the form of user instructions, the complete set of processes and procedures that are necessary to extract all online, nearline, and offline data, including, but not limited to, databases, object and file storage, system configurations, and network configurations such that any DoD customer can use these instructions to migrate data from JEDI Cloud to another environment. The transition plan must also include an explanation evidencing the ability to demonstrate successful cleansing or destruction of all system components and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once removed from JEDI Cloud.

5 Performance Metrics: The metrics defined below identify the performance requirements for JEDI Cloud. These metrics will be reviewed annually and may change as technological advances occur.

Objectives	Standard	Acceptable Quality Limit	Monitoring Method
Time to Spin Up VM, Storage, etc			
Connection speed			
Tactical Edge compute capacity / speed			

Tactical Edge storage capacity			
Continuity of Operations spin up time			
CONUS Data Storage Capacity			
OCONUS Data Storage Capacity			
“Offline” Storage solution			
Establish Classified Network			
Response time for confirmation of job submission			
Time required to go from power off to receiving user instructions			
Patch application and updates to underlying infrastructure and cloud services	Within 8 Hours of notification		

Constraints

Any constraints are provided elsewhere in the SOO or listed in the Cyber Security Plan.

Deliverables

Deliverable	Frequency	Medium/Format/# of Copies	Submit To
Kick Off Meeting	Within XX days of award		
Monthly Report	By the 15th of every month		
Transition Out Proof Plan	Within XX days of notification from Contracting Officer	Electronic copy in format TBD by COR.	Contracting Officer and COR
Contract Security Plan	Draft submitted with proposal, final plan due 30 calendar days after award. Updated as required.	Electronic copy in provider preferred format	Contracting Officer and COR
Operations and Maintenance Plan	Draft submitted with proposal, final plan due 30 calendar days after award. Updated as required.	Electronic copy in provider preferred format	Contracting Officer and COR
System Administrator Training Course	No less than 30 days after award		DoD System Administrators
User Training Course	No less than 30 days after award		DoD Users
Data Standards	No less than 7 days after award		Program Office

Application Standards	No less than 7 days after award		Program Office
Portability Plan	Within 60 days after notification from Contracting Officer		Program Office

354